FORM PTO-1390 (REV 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: 82032-00004

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1 5): 09/601232

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/09576	07 December 1999 (07.12.99)	08 December 1998 (08.12.98)

TITLE OF INVENTION

DEVICE FOR GENERATING A DESCRAMBLING SIGNAL

APPLICANT(S) FOR DO/EO/US

Andrew Augustine WAJS

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. X This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 37 1.
3. X This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. X A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. X has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. X A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. X Other items or information:

    -Courtesy copy of the International Application as published with International Search Report.

533 Rec'd PCT/PTO 31 JUL 2000

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/601232	PCT/EP99/09576	82032-00004

17. X The following fees are submitted:

	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$970.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepartd by the EPO or JPO **$840.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$690.00**		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy Provisions of PCT Article 33(1)-(4) **$670.00**		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(l)-(4) **$96.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$840.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than X 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	130 (not included) $	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	12-20 =		X $18.00	$	
Independent claims	4- 3 =	1	X $78.00	$78.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$260.00	$	

TOTAL OF ABOVE CALCULATIONS =	$918.00	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).		
SUBTOTAL =	$918.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +		
TOTAL NATIONAL FEE =	$918.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$	
TOTAL FEES ENCLOSED =	$918.00	
	Amount to be refunded:	$
	charged:	$

a. X A check in the amount of $ 918.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1349. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
HOGAN & HARTSON LLP
Celine Jimenez Crowson
555-13th Street, N.W., 7W
Washington, D.C. 20004
(202) 637-5703

SIGNATURE:

CELINE JIMENEZ CROWSON
NAME

40,357
REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Andrew A. WAJS	371 of International Application
Serial No.: **not yet assigned**	IA #: **PCT/EP99/09576**
Filed: **even date herewith**	IA Date: **07 December 1999**
Title: **DEVICE FOR GENERATING A DESCRAMBLING SIGNAL**	Atty Dkt. No.: **82032-00004**

PRELIMINARY AMENDMENT

Commisioner of Patents and Trademarks
Washington, D.C.

Sir:

Prior to calculation of the filing fee and examination on the merits, please amend the above-identified application as follows.

IN THE CLAIMS:

Claim 4, line 1, delete "or 3".

Claim 5, lines 1 and 2, change "according to any one of the preceding claims" to --claim 1--.

Claim 6, lines 1 and 2, change "according to any one of the preceding claims" to --claim 1--.

Claim 7, line 1, change "any one of claims 1-5" to --claim 1--.

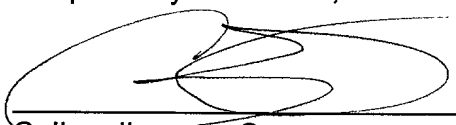
Claim 10, lines 1 and 2, change "according to any one of the preceding claims" to --claim 1--.

HOGAN & HARTSON
L.L.P.
COLUMBIA SQUARE
555 THIRTEENTH STREET NW
WASHINGTON DC 20004-1109
(202) 637-5600

REMARKS

The above amendments are being made to delete multiple dependencies in the claims and does not add to or depart from the original disclosure or constitute prohibited new matter.

Respectfully submitted,



~~Celine Jimenez~~ Crowson
Attorney for Applicant
Registration No. 40,357
Hogan & Hartson, LLP
555 13th Street, N.W., Suite 701-W
Washington, D.C. 20004
PH: 202-637-5600

HOGAN & HARTSON
L.L.P.
COLUMBIA SQUARE
555 THIRTEENTH STREET NW
WASHINGTON DC 20004-1109
(202) 637-5600

Device for generating a descrambling signal

The invention relates to a device for generating a descrambling signal.

Such a device is used in a descrambling system for descrambling a scrambled content or information signal. When the content is descrambled the clear content could be used by unauthorized persons, i.e. a pirate, for distribution or other unauthorized commercial purposes. With conventional systems for descrambling a scrambled content, it is generally impossible to trace the descrambling system or descrambling signal generating device which is used to obtain the content distributed by an unauthorized person.

The invention aims to provide a device of the above-mentioned type, wherein it is relatively easy to trace the descrambling system or descrambling signal generating device used to obtain a clear content, by means of this clear content.

To this end the device of the invention comprises a first generator providing a descrambling base signal, a second generator providing a watermark signal, and means for combining the descrambling base signal and the watermark signal into a descrambling signal, wherein the watermark signal generated by the second generator includes a device identification.

In this manner a device is obtained, wherein the descrambling signal contains a watermark signal including a device identification. This device identification will be added to the clear content during the descrambling operation and in this manner the device can be traced by analysing the clear watermarked content.

The invention will be further explained by reference to a drawing showing a descrambling system equipped with an embodiment of the device of the invention.

In the following description an embodiment of a device for generating a descrambling signal will be described as used in a descrambling system described in a co-pending patent application of the same applicant. However it is noted that the present device for generating a descrambling signal is not restricted to a device for use in such a descrambling system.

The descrambling system shown in the drawing is provided with a device for generating a descrambling signal which is preferably part of a secure device 1, such as a smart card. The descrambling signal generating device comprises a first generator 2 providing a descrambling base signal and a second generator 3 providing a watermark signal, wherein the descrambling base signal and the watermark signal are combined in an adder 4. The adder 4 provides the descrambling signal used in the descrambling system which will be described hereinafter. It is noted that the term descrambling base signal is used to refer to any conventional descrambling signal.

In the preferred embodiment, the second generator 3 comprises a pseudo random sequence generator 5 seeded by a key received from a control unit 6 of the descrambling system. The second generator 3 further comprises a device identification sequence source 7, which can be made as a memory. The identification sequence is modulated on the pseudo random sequence provided by the generator 5 by means of an exclusive or operation 8. The bit rate of the pseudo random sequence is much higher than the bit rate of the identification sequence, so that the output of the exclusive or operation 8 has a bandwith corresponding with the bit rate of the pseudo random sequence. The output of the exclusive or operation 8 is the watermark signal which is added to the descrambling signal.

The output of the adder 4 is the descrambling signal which is used to descramble the scrambled input received on an input 9. As this scrambled input has been compressed and decompressed, an equalizer or compensation filter 10 is provided to replicate the impulse response of the transfer

function of this compression and decompression steps. The equalizer 10 is adjusted by the control unit 6 to provide the correct impulse response. This is further described in the above-mentioned co-pending application. Further the output of the equalizer 10 is processed by a processor 11 in such a manner that the entropy distribution of the descrambling signal corresponds to the entropy distribution of the original scrambling signal and clear content. The processor 11 is also adjuted by the control unit 6. It is noted that information on the required settings can be received by the control unit 6 from an outside source as part of an entitlement or other control file, for example. This file can be forwarded as a separate data stream or can be inserted into the scrambled information data stream. By combining the scrambled content and the processed descrambling signal in a descrambler 12 a clear watermarked content is obtained. The decrambling system is not a part of the present invention and is described in the co-pending application which is deemed to be incorporated here by reference.

If the descrambling signal generating device is used by a pirate to obtain the clear content, this clear content will be watermarked with the device identification sequence. By analysing the content provided by the pirate, the watermark signal can be detected and in this manner the secure device 1 used by the pirate can be traced. Thereafter, the secure device can be made useless, for example by no longer using the private key of the secure device 1 for encrypting the files containing information necessary for operating the descrambling system, such as an entitlement file, the key for seeding the first generator 1 and the key for seeding the generator 5.

In order to prevent removal of the device identification sequence by combining the descrambling signals obtained from two or more descrambling signal generating devices, a processor 13 of the secure device 1 is programmed such that the phase relationship between the pseudo random sequence provided by the generator 5 and the device identification sequence provided by the source 7 is randomly se-

lected. This means that there is no fixed relationship between these two sequences if the output signals of two or more of the devices as described are combined. Averaging the output signals will then not result in a removal of the device identification sequences.

As an alternative, the processor 13 can control the exclusive or operation 8 on the device identification sequence and the pseudo random sequence such, that the device identification sequence is repetitively modulated on the pseudo random sequence, wherein at each repetition the processor 13 checks a next bit of the identification sequence and inverts all bits of the identification sequence if this checked bit has a given logic value, i.e. either a zero or a one. This means that if at the first repetition the first bit is a logic one for example, all bits are inverted. For the second repetition, the second bit is checked and if it is logic one, then the entire identification sequence is inverted, etc. Again averaging of the descrambling signals generated by the device described will not lead to removal of the device identification sequences.

If it is found that a device is used by a pirate to descramble a scrambled content for unauthorized commercial purposes, for example distribution on the internet, the provider of the descrambling signal devices, i.e. the secure devices, can trace the or each secure device used in an easy manner. For, the authorized person knows the pseudo random sequence generator used in the devices 1. By synchronising the pseudo random sequence with the watermarked content signal, the device identification sequence can be found. The manner for synchronisation corresponds with synchronisation in a spread spectrum system. Therefore, this synchronisation and detection of the watermark signal is not further described.

In case of a device as described using random selection of the phase relationship between the pseudo random sequence and the device identification sequence, it can easily be established from the symbol rate of the watermark signal how many sequences have been averaged. For, the data

rate of the device identification sequence is known to the authorized provider. If for example two identification sequences are contained in the watermarked content, it is possible to "de-multiplex" the two device identification sequences by selecting every second symbol detected for each identification sequence. Of course, first the "multiplex" of the two identification sequences is detected by synchronising the known pseudo random sequence with the watermarked clear content.

In case of devices using repeated insertion of the identification sequence into the pseudo random sequence with inversion of the bits depending on the bit value of each next bit, the identification sequences of the devices used to average out the watermark signals can be derived from the detected sequences hidden in the content. Assume for example that two devices have been used by the pirate having the identification sequences 101 and 110 and that these sequences are inserted four times with inversion of the bits as described. This means that the first device will have generated 101, 010, 101, 010, while the second device will have generated 110, 001, 001 and 110. Despite averaging these sequences, detection will provide the sequences 1xx, 0xx, x01, x10, wherein a "1" or a "0" occurs when there is coincidence of the same value and a "x" denotes an undetected symbol due to averaging out. As the provider knows the repetition and inversion scheme used, the detected sequences learn that the both sequences start with a value 1, as the first detected sequence starts with a value 1. Further, the second and third symbols of the sequences are not equal to each other. The second sequence provides no further information and the third sequence learns that the second symbol of only one identification sequence changed, so that we have 11x and 10x. The fourth detected sequence learns that the third symbol of at least one identification sequence changed again. If we assume one identification sequnce to be 101, this automatically provides 110 for the other.

It is noted that the above-described devices for

adding a watermark signal with random phase relationship or repeated insertion of the watermark signal can be used in combination with any type of descrambling signal generator or even separate from a descrambling signal generator.

A pirate could try to prevent watermark signal detection by slightly changing the bit rate of the content. As the provider knows the original bit rate of the content this type of distortion of the content to prevent watermark signal detection can be removed by comparing the bit rates of the original and pirate contents. The provider can then change the bit rate of the pirate content back to the original one and can then start one of the described detection schemes.

A further or other type of protection against unauthorized use by pirates can be obtained by using the processor 13 of the secure device 1 to add a compression hindering signal to the output of the generator 2. This compression hindering signal will then be part of the descrambling signal used by the descrambler 12 and will be inserted in this manner into the clear content on the output. The compression hindering signal for example inserts noise into the information signal which will not affect the quality of the information signal. It will however significantly affect any compression algorithm to effectively compress the information signal, so that a pirate will not be able to effectively recompress the clear content for distribution purposes. If the compression hindering signal is used independent of a descrambling signal generator, the compression hindering signal will be added to the clear content in a suitable manner.

The invention is not restricted to the above described embodiment which can be varied in a number of ways within the scope of the claims.

CLAIMS

1. Device for generating a descrambling signal, comprising a first generator providing a descrambling base signal, a second generator providing a watermark signal, and means for combining the descrambling base signal and the watermark signal into a descrambling signal, wherein the watermark signal generated by the second generator includes a device identification.

2. Device according to claim 1, wherein the watermark signal generator comprises a pseudo random sequence generator seeded by a key, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal.

3. Device according to claim 2, wherein the modulator provides an exclusive or operation on the device identification sequence and the pseudo random sequence, wherein preferably the bit rate of the pseudo random sequence is much higher than the bit rate of the device identification sequence.

4. Device according to claim 2 or 3, wherein the key delivered to the pseudo random sequence generator is received from an outside source.

5. Device according to any one of the preceding claims, comprising a generator for generating a compressing hindering signal and means for inserting the hindering signal into the descrambling signal.

6. Device according to any one of the preceding claims, comprising a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the phase relationship between the pseudo random sequence and the device identification sequence is randomly selected.

7. Device according to any one of claims 1-5, comprising, a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the device identification sequence is repetitively modulated on the pseudo random sequence, wherein at each repetition a control unit checks a next bit of the device identification sequence and inverts the bits of the device identification sequence if this bit has a given logic value.

8. Device for generating a watermark signal, comprising a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the phase relationship between the pseudo random sequence and the device identification sequence is randomly selected.

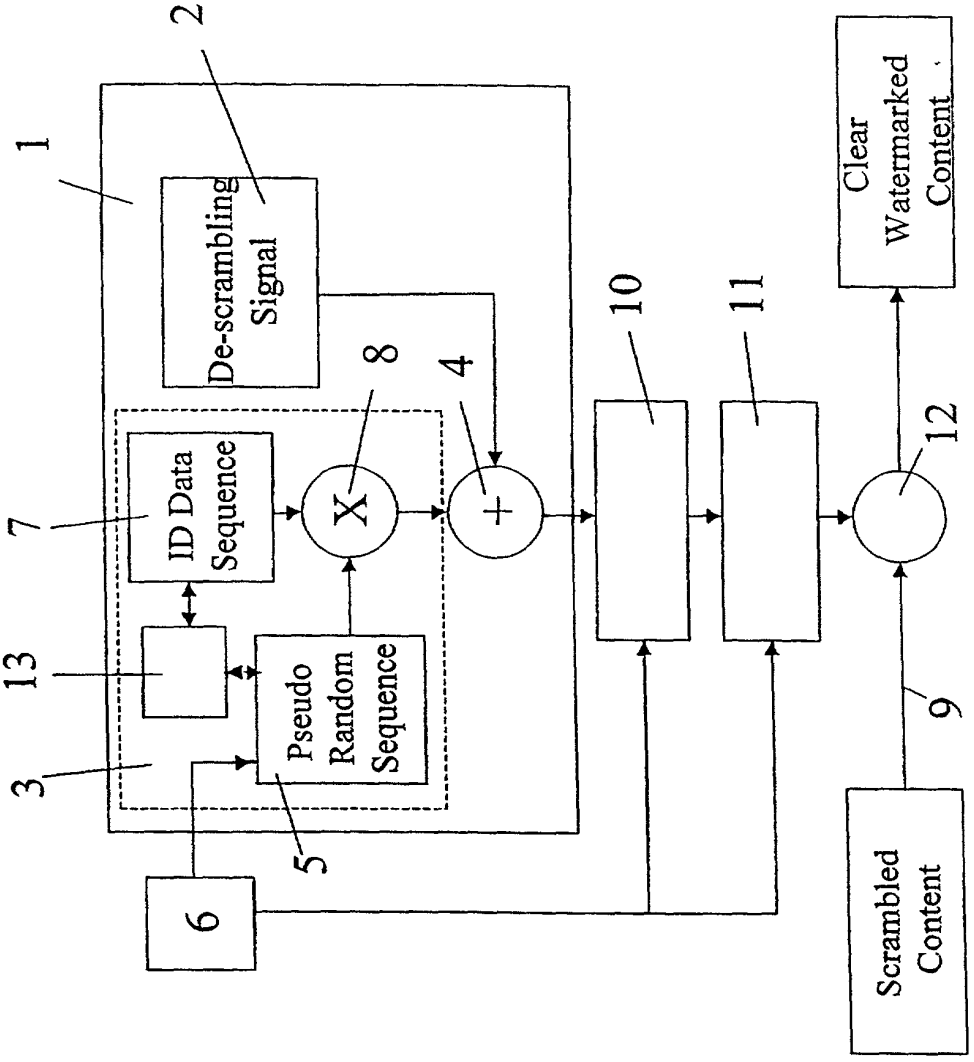
9. Device for generating a watermark signal, comprising a pseudo random sequence generator, a device identification sequence source, and a modulator, wherein the device identification sequence provided is modulated on the pseudo random sequence to obtain the watermark signal, wherein the device identification sequence is repetitively modulated on the pseudo random sequence, wherein at each repetition a control unit checks a next bit of the device identification sequence and inverts the bits of the device identification sequence if this bit has a given logic value.

10. Device according to any one of the preceding claims, wherein the device is implemented in a secure device, such as a smart card.

11. System to detect a watermark signal hidden in an information signal, comprising a pseudo random signal generator, means for synchronising the pseudo random signal generator and the information signal, means for detecting a data sequence hidden in the information signal and for determining the number (n) of watermark signals in the hidden data sequence and means for selecting every n^{th} bit from the

detected hidden data sequence as bits of one of the n watermark signals.

12. System according to claim 11, wherein said means for determining the number (n) of watermark signals comprises means for detecting the bit rate of the hidden data sequence and comparing the detected bit rate with the known bit rate of one watermark signal.


1
2
De-scrambling Signal
8
4
7
ID Data Sequence
X
+
10
11
Clear Watermarked Content
12
13
Pseudo Random Sequence
3
5
9
6
Scrambled Content

Docket No. 82032-00004

Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought, on the invention entitled DEVICE FOR GENERATING A DESCRAMBLING SIGNAL, the specification of which was filed as U.S. Application No. 09/601,232, filed July 31, 2000.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

			Priority Claimed
98204136.0	Europe	08 December 1998	[x] [ ]
(Number)	(Country)	(Day/Month/Year)	Yes No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

_____ _____

(Application Serial No.) (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred

between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status)
PCT/EP99/09576	07 December 1999	

I or we hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed to HOGAN & HARTSON L.L.P., 555 13th Street, N.W., Washington, D.C. 20004

Celine Jimenez Crowson, Reg. No. 40,357 (2)
Kevin G. Shaw, Reg. No. 43,110

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

FIRST NAMED INVENTOR	SIGNATURE	DATE
Andrew Augustine Wajs		8/9/00
RESIDENCE	CITIZENSHIP	
NL-2023 AA Haarlem	Great Britain/The Netherlands	
POST OFFICE ADDRESS	NLX	
Schotersingel 93, NL-2023 AA Haarlem, The Netherlands		